Security Area Concepts

At Battalion and Brigade

LIEUTENANT COLONEL JACK E. MUNDSTOCK

Security area operations are critical to the success of any defensive battle. The tempo of operations and the probability of success are all tied up in the conduct of the security area battle. Too often, commanders and their staffs see the security area as a relatively unimportant part of the defensive fight. In most battles, however, the security area fights alone may determine the outcome or, at the very least, directly affect success. Although this article discusses security area concepts primarily at the brigade and battalion level, applications for these ideas can be found at all levels.

In a broad sense, the responsibilities of the security area can be summarized in four words: *disrupt*, *delay*, *deceive*, and *destroy*.

The *disrupt* function is primarily to keep the enemy off his timeline; for example, prevent him from accurately locating defensive positions or setting his artillery in the most advantageous positions to support his attack.

The *delay* function is tied to the doctrinal definition in Field Manual (FM) 101-5-1, *Operational Terms and Symbols*, but I do not mean to imply that every security area has a delay mission. Regardless of the mission assigned to the security area, the result must be to slow the enemy enough to apply effective fires to his formations and to allow the higher commander to reposition reserves or MBA forces to counter the enemy attack.

The *deceive* function is one that has been the purpose of security forces throughout history. The security area should keep the enemy guessing about where the MBA begins and perhaps cause him to deploy into assault formations earlier than planned. The security area should also reinforce the tactical concept of the MBA, making it more effective. Specifically, this means that if the commander's intent is to fight the enemy in one particular portion of his sector, then the security area should begin the process of influencing the enemy to go to that place.

The *destroy* function is also necessary to the success of the security area. No matter what mission is assigned to the security force, it will destroy some portion of the enemy and it must do so in a fashion that allows the security unit to remain combat effective. Destroying a platoon-sized element will require a company team; destroying a company sized unit will require a battalion task force. Even in a *screen* mission for a battalion, the security force will probably be tasked to destroy individual vehicles or observation posts (OPs).

The term *destroy* has different meanings in different military communities, and the commander must ensure that his subordinates understand what he wants them to do. Any tactical tasking involving the term "destroy" should have exact numbers or percentages associated. The lack of this guidance is sure to create ambiguity.

Battalions and brigades will conduct primarily *screen* or *guard* missions. The third option, the *cover* mission, is normally conducted by an armored cavalry regiment, an entire brigade, or possibly a heavily reinforced cavalry squadron. The other possible security mission is *area* security, which again is not normally conducted by a brigade or battalion. The commander will determine the form of security to be conducted, on the basis of a number of factors. A screen may be the choice when there is a shortage of time, there are limited avenues of approach for the enemy, or the commander wants to retain most of his combat power for the MBA fight. The *guard* mission may be the choice if there are multiple avenues of approach and enough time to execute a detailed obstacle plan, and if the commander has enough combat power to commit a sizable portion of it to the security area. These choices will be discussed in more detail.

Counterreconnaissance is not a mission; it is one of the results of a security operation. In almost every case, the security area has to do more than defeat the enemy reconnaissance elements. In the most basic form of security—the screen—the security force must maintain contact with the enemy's forward security element (FSE), which is not a reconnaissance asset. There is no doubt that destroying or reducing the enemy reconnaissance assets is an important task, but opposing force (OPFOR) doctrine directs that lost reconnaissance elements be reconstituted and that the security area do more to ensure the success of the defense. Generally, it is a mistake to concentrate solely on the enemy reconnaissance elements and neglect the rest of the oncoming enemy force.

The *screen* and *guard* definitions include a list of critical tasks to be performed. The commander and his staff must ensure that the unit conducting the security area mission understands which of these tasks it is required to execute. Missions that are as potentially broad as security area missions can be, must be focused so those subordinate units can concentrate on exactly what the commander wants to have accomplished.

Intelligence

The key areas of intelligence are that the staff must have developed solid enemy situational templates and event templates as part of the general intelligence preparation of the battlefield (IPB) process. The situational template shows the predicted echelonment of the entire enemy force and may show possible task organization for subordinate units. The event template or predicted enemy timeline shows when each enemy element could reach a designated phase line, usually the forward edge of the battle area (FEBA). These products are doubly crucial in that a staff could not have conducted an adequate war game without them and needs them for conducting the defensive mission.

The commander and his entire staff, not just the S-2, must have a working knowledge of enemy doctrine and use that knowledge to trigger necessary responses. As an example, the OPFOR that we train against usually employs an FSE as a lead element for its main attack. When the FSE is identified in the security area, this should be an event that the staff is looking for, and should probably initiate a series of responses from the commander to alter the configuration of the MBA.

Command and Control

The command and control and maneuver battlefield operating systems (BOSs) tend to blur at times, and even people who often deal with the terms have some difficulty distinguishing between them. This section will address both the maneuver and the command and control aspects of the security area missions.

Once the commander has chosen the form of security he wants to conduct, a decision must be made as to whether the security area will be under his control or delegated to a subordinate formation. There are advantages and disadvantages to having the security area as a higher level responsibility—that is, under the control of whatever headquarters, battalion, or brigade is conducting the defense. Centralized control allows a more focused application of fires and obstacles, as examples, but gives that commander one more sector or unit to command directly. An example of maintaining centralized control would be to have two units defending in the MBA and a third unit forward in the security area. This forward unit has a follow-on mission to be the reserve or to defend in depth from a subsequent position after battle handoff with the MBA (Figure 1), one up and two back, transitioning to two up and one back. A unit defending in the classic two up and one back (Figure 2) could split the security area responsibility between the two forward elements, extending their sectors to the forward line of own troops (FLOT). A considerable advantage to this method is that battle hand-off would be between units of the same battalion, which should make it smoother.

Splitting the responsibility for the security area can result in two different approaches to what should be a unified vision. Generally speaking, the best results are achieved with a centralized security area, conducting a guard mission with adequate combat power. This does not mean that units should never do a screen. The primary problems with the screen mission are that commanders and their staffs do not give the security force a clear mission and adequate resources. This is caused by a failure to analyze exactly what it is that they want the screening force to do and give guidance to their subordinates.

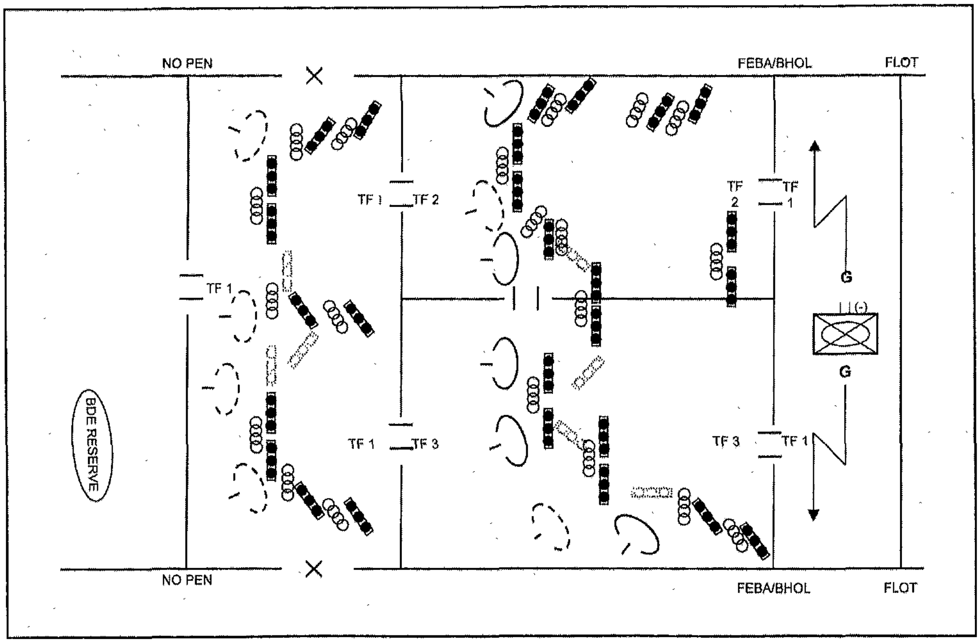

Figure 1

An example of a tasking to a company team conducting a screen is, "Team A conducts a screen from phase line Alpha to phase line Bravo to destroy (100%) division reconnaissance and brigade reconnaissance; attrit by one-third the combat reconnaissance patrols (CRPs); maintain contact with the FSE; on order, conduct battle handoff with the MBA and move to battle position (BP) Dog to become the task force reserve." With a little refinement, this could be the mission statement for that unit. It is obvious that this is a very complex tasking and will need a good company commander to execute. The key point is that commanders have to recognize the complexity and ensure that this unit has the force resources to conduct the mission.

An example of a tasking to a guard is, "TF 1-999(–) conducts a guard from phase line Alpha to phase line Bravo, to destroy (100%) the division reconnaissance and brigade reconnaissance, CRPs; destroy (by 75%) the FSE; attrit by one-third the advance guard main body (AGMB); on order, conduct battle hand-over with TF 1-998 and TF 1-997, move to BP Red to defend in depth in the brigade sector." Obviously, a lot is going on here, and it may be too much for one unit to execute. A guard force with the ability to execute these tasks would have given the commander the opportunity to reposition MBA forces or create situational obstacles, as the enemy scheme of maneuver would be obvious due to the successful execution of the security area mission. The intent was to show the kind of clear guidance that has to be issued to conduct a security area mission. There is no intent to imply that only a battalion task force can conduct a guard mission. A company team could conduct a guard, although obviously in a smaller area.

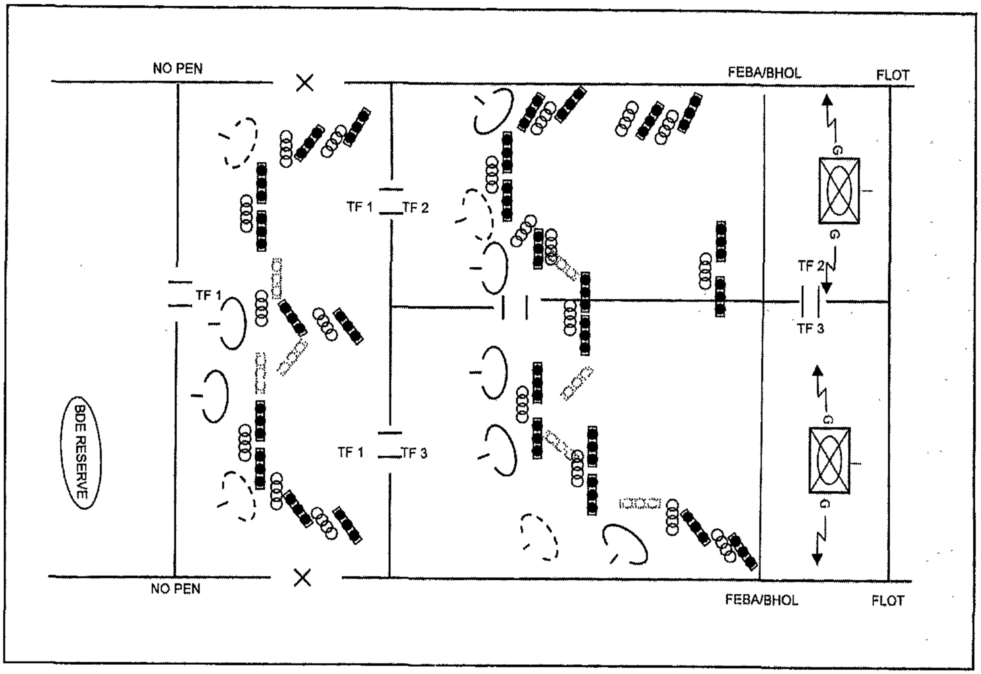

Figure 2

No matter which mission is executed in the security area or how the command and control responsibility is divided, the battle hand-over between the security area and the MBA is critical. The commander has to ensure that the engagement of the enemy is seamless between the two areas, while extracting the security area force to a subsequent position or mission. This effort will be further complicated by the fact that only one portion of the security area may be in heavy contact, making it unclear (and maybe unnecessary) to withdraw the entire security area force. In such a situation, one part of the security area may be withdrawn, while the rest stays in place, perhaps requiring a change in the command and control relationship in the security area. The successful execution of the defense will demand a flexible plan and almost certainly the movement of units from one subordinate headquarters to another. This will take place during the fight as well as before it. The first task organization changes on the fly will probably be made in the security area.

Fire Support

The fastest way to concentrate combat power is through the fire support BOS. What often happens is that a commander and his staff do not adequately meet the needs of the security area unit. It would seem obvious that the security area would receive the initial priority of fires. Frequently, the positioning of the artillery firing units is not cross-checked with the range requirements of the security area. If the indirect fires are to be truly effective, they must be fully integrated with the direct fire plan and the obstacle plan.

When a unit is conducting a screen, the commander generally intends that most of the enemy engagement be with indirect fire, as this puts the security force at the minimum risk while allowing very effective fire to be placed on the enemy. The fire support units themselves must be maneuvered during this process. In most cases, the best positions for the artillery or mortars to support the security area are not the same ones they must be in to support the MBA fight. The responsibility for coordinating this movement rests with the staff, and the principal reason it does not happen is that the requirement was not recognized during the decision making process, specifically during war gaming.

The requirements for counter-fire radar coverage are also overlooked, as leaders outside the artillery community generally do not recognize the range or accuracy of the Q36 and Q37 radars. The security area should be allocated a reasonable number of critical friendly zones (CFZs) to be used in the counterfire program. Most units do not use these zones at all, and the artillery battalion ends up either placing them on their firing batteries or not using them at all.

Assuming that the commander has decided to use and allocate artillery final protective fires (FPFs) and/or priority targets, it is important that the security area force get a reasonable share of these assets. The priority targets could be used to engage an important target with preplanned fires, while the FPFs could aid in the displacement of the force when ordered to conduct battle hand-over with the MBA units.

Countermobility and Survivability

When the commander and staff are planning and executing the obstacle portion of the defensive concept, the security area often gets too few of the assets. There is almost always an obstacle intent to be executed in the security area, and the security force commander must receive the appropriate amount of class IV/V obstacle materiel and the engineer platoon hours to accomplish the task.

In order for the security area mission to succeed, the obstacle intent must accomplish at least three things: allow the security force to place accurate effective *indirect* fires on the enemy, allow the security force to place accurate *direct* fires on the enemy, and assist the security force in conducting a battle hand-over with the MBA task forces. The obstacle intent for the security area is the senior commander's responsibility; he will either establish it for the security area commander or approve the intent as part of the overall concept presented by the security area commander.

The priority of work must be approved by the commander with all the implications fully explained by the staff. Generally, we work from front to rear—beginning in the security area and then working in the MBA. The obvious reason for this is that the security area will engage the enemy first.

Air Defense

When the force for the security area is task organized, the air defense portion tends to be overlooked. This leads to some obvious problems when enemy air assets show up, even if they are only reconnaissance aircraft. The first thing—which should have been determined during the wargaming—is whether or not the Patriot or other air defense coverage will extend into the security area; sometimes it does not. The security area will benefit greatly from the early warning feeds that go to the air defense units. Although this information may be available from other sources, units have a lot of problems getting the early warning nets to work on the command net or other nondedicated frequencies. The time when the security force will be the most vulnerable to air attack is during battle hand-over with the MBA when the bulk of the area force will be moving.

Combat Service Support

The CSS assets will definitely earn their money during a security area mission. The commander and staff have to track a number of things and conduct considerable planning with the forward support battalion (FSB).

The plan to support the security area obstacle effort must be airtight. There is almost always a shortage of time, and this can be worse when all the needed materiel is not where it should be. The security area units should be allocated a class IV/V supply point for their obstacle materiel needs. The designation of this point and the responsibility for running it is a command issue, not a CSS or an engineer issue, although those operating systems do have a vested interest in what goes on there. The FSB must ensure that materiel handling equipment is on hand to move some extremely heavy and bulky items from the supply point to the site where the obstacles will be emplaced. Engineers should not constitute the work force at the supply point; their time is better spent on the obstacles themselves. The packages of obstacle materiel should have been pre-configured, probably at corps level, and sent as a corps through-put to the supply point. In order to ensure that the corps trucks get to the right place, a first destination release point (FDRP) should be established and the corps trucks led forward from this location to the security area IV/V supply point. The FDRP is usually established at the brigade support area (BSA), and this same procedure would be used for the rest of the defense as well.

The casualty evacuation plan will stretch the medical community. A solid casualty evacuation plan will include the use of helicopters for the critical patients, and a robust ground evacuation plan, as the enemy air defense may prevent the helicopters from flying. It may even be necessary to plan for indirect fires to suppress enemy air defense missions. The commander and staff cannot allow the briefing of the evacuation assets only; they must understand the plan and be confident that it will work.

The security area commander should plan on removing all non-critical CSS assets from the area so that they do not impede the battle, the subsequent battle hand-over, or movement to a new mission. These assets could then form the advance party at the new location.

The security area is one aspect of the defense—the hardest thing to do tactically. The defense is difficult primarily because the initiative rests with the attacker, and he will determine when the action begins. The commander and his staff must understand exactly what the security area force is to do and ensure that it has the resources to execute according to his intent. The security area has to contribute to the one thing every defender wants—to wrest the initiative from the enemy, thereby setting the conditions to attack and destroy him.

Lieutenant Colonel Jack E. Mundstock is combat arms advisor, 28th Field Training Group, 28th Infantry Division, Pennsylvania Army National Guard. He previously served as maneuver BOS chief, and Chief OT, Operations Group C, BCTP, and in the 1st Ranger Battalion, the 7th Special Forces Group (A), the 3d Armored Division, and the 82d Airborne Division. He is a 1975 ROTC graduate of Marshall University.